United States General Accounting

GAO

Testimony

Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at
10:00 a.m. EDT
Tuesday,
May 22, 2001

CRITICAL INFRASTRUCTURE PROTECTION

Significant Challenges in Developing Analysis, Warning, and Response Capabilities

Statement of Robert F. Dacey
Director, Information Security Issues

G A O

Accountability * Integrity * Reliability

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our review of the National Infrastructure Protection Center (NIPC). As you know, the NIPC is an important element of our government's strategy to protect our national infrastructures from hostile attacks, especially computer-based attacks. This strategy was outlined in Presidential Decision Directive (PDD) 63, which was issued in May 1998.

My statement summarizes the key findings in our report on the NIPC, which you have released today.[1] That report is the result of an evaluation we performed at the request of you, Mr. Chairman; Senator Feinstein; and Senator Grassley. As you requested, the report describes the NIPC's progress in developing national capabilities for analyzing cyber threats and vulnerability data and issuing warnings, enhancing its capabilities for responding to cyber attacks, and establishing information-sharing relationships with government and private-sector entities.

Overall, progress in developing the analysis, warning, and information-sharing capabilities called for in PDD 63 has been mixed. The NIPC has initiated a variety of critical infrastructure protection efforts that have laid a foundation for future governmentwide efforts. In addition, it has provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, the analytical and information-sharing capabilities that PDD 63 asserts are needed to protect the nation's critical infrastructures have not yet been achieved, and the NIPC has developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort. A underlying contributor to the slow progress is that the NIPC's roles and responsibilities have not been fully defined and are not consistently interpreted by other entities involved in the government's broader critical infrastructure protection strategy. Further, these

[1] *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

entities have not provided the information and support, including detailees, to the NIPC that was envisioned by PDD 63.

The NIPC is aware of the challenges it faces and has taken some steps to address them. In addition, the administration is reviewing the federal critical infrastructure protection strategy, including the way the federal government is organized to manage this effort. Our report includes a variety of recommendations that are pertinent to these efforts, including addressing the need to more fully define the role and responsibilities of the NIPC, develop plans for establishing analysis and warning capabilities, and formalize information-sharing relationships with private-sector and federal entities.

The remainder of my statement will describe the NIPC's role in the government's broader critical infrastructure protection efforts, as outlined in PDD 63, and its progress in three broad areas: developing analysis and warning capabilities, developing response capabilities, and establishing information-sharing relationships.

Background

Since the early 1990s, the explosion in computer interconnectivity, most notably growth in the use of the Internet, has revolutionized the way organizations conduct business, making communications faster and access to data easier. However, this widespread interconnectivity has increased the risks to computer systems and, more importantly, to the critical operations and infrastructures that these systems support, such as telecommunications, power distribution, national defense, and essential government services.

Malicious attacks, in particular, are a growing concern. The National Security Agency has determined that foreign governments already have or are developing computer attack capabilities, and that potential adversaries are developing a body of knowledge about U.S. systems and methods to attack them. In addition, reported incidents have increased dramatically in recent years. Accordingly, there is a growing risk that terrorists or hostile foreign states

could severely damage or disrupt national defense or vital public operations through computer-based attacks on the nation's critical infrastructures. Since 1997, in reports to the Congress, we have designated information security as a governmentwide high-risk area. Our most recent report in this regard, issued in January,[2] noted that, while efforts to address the problem have gained momentum, federal assets and operations continued to be highly vulnerable to computer-based attacks.

To develop a strategy to reduce such risks, in 1996, the President established a Commission on Critical Infrastructure Protection. In October 1997, the commission issued its report,[3] stating that a comprehensive effort was needed, including "a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyber threats." The report said that the Federal Bureau of Investigation (FBI) had already begun to develop warning and threat analysis capabilities and urged it to continue in these efforts. In addition, the report noted that the FBI could serve as the preliminary national warning center for infrastructure attacks and provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

In May 1998, PDD 63 was issued in response to the commission's report. The directive called for a range of actions intended to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious computer-based attacks. The directive established a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism under the Assistant to the President for National Security Affairs. Further, the directive designated lead agencies to

[2] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997); *High-Risk Series: An Update* (GAO/HR-99-1, January, 1999); *High-Risks Series: An Update* (GAO-01-263, January 2001).

[3] *Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection,* October 1997.

work with private-sector entities in each of eight industry sectors and five special functions. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and the Department of Energy is responsible for working with the electric power industry.

PDD 63 also authorized the FBI to expand its NIPC, which had been originally established in February 1998. The directive specifically assigned the NIPC, within the FBI, responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to cyber incidents; providing law enforcement investigation and response; monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing.

Multiple Factors Have Limited Development of Analysis and Warning Capabilities

PDD 63 assigns the NIPC responsibility for developing analytical capabilities to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities as well as timely warnings of potential and actual attacks. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is underway or imminent.

Since its establishment in 1998, the NIPC has issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. These analyses have included (1) situation reports related to law enforcement investigations, including denial-of-service attacks that affected numerous Internet-based entities, such as eBay and Yahoo and (2) analytical support of a counterintelligence investigation. In addition, the NIPC has issued a a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis.

Strategic analysis to determine the potential broader implications of individual incidents has been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

Three factors have hindered the NIPC's ability to develop strategic analytical capabilities.

- First, there is no generally accepted methodology for analyzing strategic cyber-based threats. For example, there is no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.
- Second, the NIPC has sustained prolonged leadership vacancies and does not have adequate staff expertise, in part because other federal agencies had not provided the originally anticipated number of detailees. For example, as of the close of our review in February, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of the NIPC's 3-year existence. In addition, the NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities.
- Third, the NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work in February, only three industry assessments had been partially completed, and none had been provided to the NIPC.

To provide a warning capability, the NIPC established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. As of February, the unit had

issued 81 warnings and related products since 1998, many of which were posted on the NIPC's Internet web site. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks underway. The NIPC's ability to issue warnings promptly is impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) a shortage of skilled staff, (3) the need to ensure that the NIPC does not raise undue alarm for insignificant incidents, and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

However, I want to emphasize a more fundamental impediment. Specifically, evaluating the NIPC's progress in developing analysis and warning capabilities is difficult because the federal government's strategy and related plans for protecting the nation's critical infrastructures from computer-based attacks, including the NIPC's role, are still evolving. The entities involved in the government's critical infrastructure protection efforts do not share a common interpretation of the NIPC's roles and responsibilities. Further, the relationships between the NIPC, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council are unclear regarding who has direct authority for setting NIPC priorities and procedures and providing NIPC oversight. In addition, the NIPC's own plans for further developing its analytical and warning capabilities are fragmented and incomplete. As a result, there are no specific priorities, milestones, or program performance measures to guide NIPC actions or provide a basis for evaluating its progress.

The administration is currently reviewing the federal strategy for critical infrastructure protection that was originally outlined in PDD 63, including provisions related to developing analytical and warning capabilities that are currently assigned to the NIPC. Most recently, on May 9, the White House issued a statement saying that it was working with federal agencies and private industry to prepare a new version of a "national plan for cyberspace security

and critical infrastructure protection" and reviewing how the government is organized to deal with information security issues.

Our report recommends that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategic analysis of computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data;
- require development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and
- clearly define the role of the NIPC in relation to other government and private-sector entities.

NIPC Coordination and Technical Support Have Benefited Investigative and Response Capabilities

PDD 63 directed the NIPC to provide the principal means of facilitating and coordinating the federal government's response to computer-based incidents. In response the NIPC has undertaken efforts in two major areas: providing coordination and technical support to FBI investigations and establishing crisis management capabilities.

First, the NIPC has provided valuable coordination and technical support to FBI field offices, which have established special squads and teams and one regional task force in its field offices to address the growing number of computer crime cases. The NIPC has supported these investigative efforts by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases, (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks, and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for the NIPC field squads and teams.

While these efforts have benefited investigative efforts, FBI and NIPC officials told us that increased computer capacity and data transmission capabilities would improve their ability to promptly analyze the extremely large amounts of data that are associated with some cases. In addition, FBI field offices are not yet providing the NIPC with the comprehensive information that NIPC officials say is needed to facilitate prompt identification and response to cyber incidents. According to field office officials, some information on unusual or suspicious computer-based activity has not been reported because it did not merit opening a case and was deemed to be insignificant. The NIPC has established new performance measures related to reporting to address this problem.

Second, the NIPC has developed crisis management capabilities to support a multiagency response to the most serious incidents from the FBI's Washington, D.C., Strategic Information Operations Center. Since 1998, seven crisis action teams have been activated to address potentially serious incidents and events, such as the Melissa virus in 1999 and the days surrounding the transition to the year 2000, and related procedures have been formalized. In addition, the NIPC has coordinated development of an emergency law enforcement plan to guide the response of federal, state, and local entities.

To help ensure an adequate response to the growing number of computer crimes, we are recommending that the Attorney General, the FBI Director, and the NIPC Director take steps to (1) ensure that the NIPC has access to needed computer and communications resources and (2) monitor implementation of new performance measures to ensure that field offices fully report information on potential computer crimes to the NIPC.

Progress in Establishing Information-Sharing Relationships Has Been Mixed

Information sharing and coordination among private-sector and government organizations are essential to thoroughly understanding cyber threats and quickly identifying and mitigating attacks. However, as we testified in July 2000,[4] establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult.

NIPC efforts in this area have met with mixed success. For example, the InfraGard Program, which provides the FBI and the NIPC with a means of securely sharing information with individual companies, has gained participants. In January 2001, NIPC officials announced that 518 organizations had enrolled in the program, which NIPC officials view as an important element in building trust relationships with the private sector. However, of the four information sharing and analysis centers that had been established as focal points for infrastructure sectors, a two-way, information-sharing partnership with the NIPC had developed with only one—the electric power industry. The NIPC's dealings with two of the other three centers primarily consisted of providing information to the centers without receiving any in return, and no procedures had been developed for more interactive information sharing. The NIPC's information-sharing relationship with the fourth center was not covered by our review, because the center was not established until mid-January 2001, shortly before the close of our work.

Similarly, the NIPC and the FBI had made only limited progress in developing a database of the most important components of the nation's critical infrastructures—an effort referred to as the Key Asset Initiative. While FBI field offices had identified over 5,000 key assets, the entities that own or control the assets generally had not been involved in identifying them. As a result, the key

[4] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation* (GAO/T-AIMD-00-268, July 26, 2000). Testimony before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives.

assets recorded may not be the ones that infrastructure owners consider to be the most important. Further, the Key Asset Initiative was not being coordinated with other similar federal efforts at the Departments of Defense and Commerce.

In addition, the NIPC and other government entities had not developed fully productive information-sharing and cooperative relationships. For example, federal agencies have not routinely reported incident information to the NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's Federal Computer Incident Response Capability. Further, NIPC and Defense officials agreed that their information-sharing procedures need improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts.

The NIPC has been more successful in providing training on investigating computer crime to government entities, which is an effort that it considers an important component of its outreach efforts. From 1998 through 2000, the NIPC trained about 300 individuals from federal, state, local, and international entities other than the FBI. In addition, the NIPC has advised five foreign governments that are establishing centers similar to the NIPC.

To improve information sharing, we are recommending that the Assistant to the President for National Security Affairs

- direct federal agencies and encourage the private sector to better define the types of information necessary and appropriate to exchange in order to combat computer-based attacks and to develop procedures for performing such exchanges,
- initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already underway, and
- resolve discrepancies in requirements regarding computer incident reporting by federal agencies.

We are also recommending that the Attorney General task the FBI Director to

- formalize information-sharing relationships between the NIPC and other federal entities and industry sectors and
- ensure that the Key Asset Initiative is integrated with other similar federal activities.

- - - - - - - - - - -

In conclusion, it is important that the government ensure that our nation has the capability to deal with the growing threat of computer-based attacks in order to mitigate the risk of serious disruptions and damage to our critical infrastructures. The analysis, warning, response, and information-sharing responsibilities that PDD 63 assigned to the NIPC are important elements of this capability. However, as our report shows, developing the needed capabilities will require overcoming many challenges. Meeting these challenges will not be easy and will require clear central direction and dedication of expertise and resources from multiple federal agencies, as well as private sector support.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

Contact and Acknowledgments

If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by e-mail at *daceyr@gao.gov.*

(310121)